CyberX XSense, un occhio vigile sulla rete di automazione

XSense traccia un identikit della rete di automazione e segnala sia ingressi di pacchetti di dati dall'esterno – possibili sorgenti di virus e malware – sia anomalie nel traffico dati interno

La crescente interconnessione dei sistemi aziendali e l'introduzione di un numero di nodi di rete sempre maggiore non sono state finora accompagnate da un'adeguata modifica dei sistemi di protezione degli asset aziendali. Impresa, del resto, niente affatto agevole perché, se da un lato crescono le minacce dall'esterno, è pur vero che nel 42% dei casi il rischio arriva dall'interno delle organizzazioni. In questa cifra rientrano i **sabotaggi**, ma anche gli **errori** degli operatori dovuti a scarsa competenza oppure a sistemi di interfacciamento non chiari o ancora i problemi derivanti da malfunzionamenti o da non accurata integrazione delle reti IT/OT. Installare un buon **firewall**, insomma, potrebbe non essere sufficiente.
La protezione dalle nuove minacce informatiche richiede senza dubbio un salto culturale che le aziende italiane, soprattutto quelle di dimensioni piccole o medie, ancora non hanno compiuto.

Tuttavia la tecnologia può dare un aiuto ed è il caso delle soluzioni proposte da CyberX, azienda distribuita e supportata in Italia da ServiTecno. La sua soluzione, denominata **XSense** è costituita da un apparato di rete e una dotazione software. Una volta collegata alla rete aziendale, XSense identifica rapidamente ogni singolo nodo che vi prende parte, dal PLC agli SCADA ai client, e ne traccia i **collegamenti**. XSense è infatti in grado di leggere i dati trasmessi con tutti i principali protocolli utilizzati in ambito industriale: Ethernet/IP, Modbus, Profinet ecc.
In tal modo il tool disegna una vera e propria mappa della rete e ne esamina il traffico in maniera passiva, senza quindi incidere in alcun modo sulle **performance** di trasmissione dei dati. Qui entra in gioco l'operatore, che definisce le regole necessarie a determinare quali siano le operazioni normalmente autorizzate. A questo punto il sistema funziona in totale autonomia e segnala all'operatore non solo eventuali ingressi di pacchetti di dati dall'**esterno** – possibili sorgenti di virus e malware – ma anche eventuali anomalie nel traffico dati **interno**, che potrebbero rivelare operazioni inusuali da parte di operatori o sistemi presenti legittimamente in rete.

L’analisi avanzata sui flussi sul traffico registrati da XSense, in altre parole, fornisce all’utente la **visibilità** e la **comprensione** necessari a gestire la sicurezza della rete di fabbrica, rilevando ogni anomalia (*anomaly detection*).
Il sistema XSense è semplice da utilizzare: un cruscotto operativo consente agli utenti di amministrare con facilità la sicurezza informatica e di gestire gli incidenti operativi. Il sistema fornisce all’utente **avvisi, analisi e diagnostica** e una serie di tool per la corretta gestione dell’infrastruttura. Il cruscotto presenta gli alert in maniera aggregata per guidare gli utenti al fine di eseguire analisi in tempo reale degli incidenti.